

A1 wherein said decoding means and said encryption means are arranged in a firmware [consisting of] including said first firmware and said second firmware in form of a composite unit; and

wherein only said first firmware has authority to access the first storage medium driven by said first drive, and only said second firmware has authority to access the second storage medium driven by said second drive.

Please **ADD** claim 8 as follows:

Sub B2 8. (NEW) A license devolution method, comprising storing in a first storage medium contents encrypted with a predetermined key, a first media ID identifying the first storage medium, and encryption secure information generated by encrypting with the first media ID the key and a first use information, which represents a right to use the contents;

2 A decoding the first encryption secure information using the first media ID to obtain the key and the first use information;

generating a second encryption secure information by encrypting with a second media ID, which identifies a second storage medium, the key and a second use information, which represents a second right to use the contents that is devolved from the first storage medium to the second storage medium; and

storing the second encryption secure information in said second storage medium, wherein the right to use the contents stored in the first storage medium is devolved from the first storage medium to the second storage medium.

REMARKS

In the Office Action mailed April 26, 2000 the Examiner objected to the specification because of informalities; claims 1-7 were rejected under 35 USC 112, first paragraph, as being

indefinite; and claims 1-7 were rejected under 35 USC 102(b) as being anticipated by Ross (US Patent No. 5,553,139).

The foregoing objections and rejections are respectfully traversed.

In the Office Action mailed April 26, 2000 the Examiner noted that claims 1-7 were pending, and rejected claims 1-7. Claims 1-7 have been amended, new claim 8 has been added, and, thus, in view of the forgoing claims 1-8 remain pending for reconsideration which is requested.

No new matter has been added in this Amendment.

SPECIFICATION

The specification, taking the Examiner's comments into consideration, has been amended to correct typographical errors and to improve English grammar. Withdrawal of the objection is respectfully requested.

CLAIM REJECTIONS

35 USC 112, first paragraph, claim rejections

Rejected claims 1-7, taking the Examiner's comments into consideration, have been amended to improve form only and not for overcoming the Examiner's rejections based upon the foregoing references. Withdrawal of the rejection of claims 1-7 is respectfully requested.

35 USC 102(b) claim rejections

Ross

Ross discloses a method and apparatus for electronic license distribution. The system in Ross provides the ability to distribute multiple products, product versions, product features, and licenses that are unusable prior to the execution of an enablement procedure. The system

in Ross requires an enabler key that is used along with an enablement software to enable a license for use (i.e., to enable the purchased products). Ross discloses that after an electronic license has been created and a portion of the license encrypted, the system in Ross disables the license for distribution (i.e., doubly-encrypted) using a special encryption algorithm that is applied to the encrypted portion of a license. An enabler key is created during the encryption process. The enabler key may comprise a serial number. In particular, the enabler key is stored in an enabler key database that is shipped to a fulfillment agent (e.g., an extractor or other member of the distribution chain). An installer of the product (i.e., enduser or other installer) obtains the enabler key from the fulfillment agent either electronically or via a voice operator. *See*, Ross, column 3, lines 14-67 and column 4, lines 1-5.

Further, in the distribution process of Ross, the doubly encrypted portion of a license is again encrypted using an extractor's password (i.e., creating a disabled license). An extractor is a reseller such as a manufacturer, original equipment manufacturer or another reseller. Disabled licenses are shipped to the extracting agent. An extractor can decrypt the extractor encryption from the license using the extractor password, which results in a disabled (i.e., doubly-encrypted) license. Disabled licenses are packaged with the products and shipped to an installer.

The system in Ross may be used in a network or non-networked environment to facilitate product licensing and upgrades. Further the system in Ross accommodates the use of compact disk read-only memory (CD-ROM) product distribution.

Claim Recitations of the Present Invention

In contrast to Ross, the present invention (as recited in independent claim 1 and new independent claim 8 directed to a method according to the present invention, using the recitation of claim 1 as an example) is directed to a license devolution apparatus that accesses a first storage medium storing "contents encrypted with a predetermined key", "a first media ID identifying the first storage medium", and "a first encryption secure information generated by encrypting the key and a first use information". The license devolution apparatus also accesses

"a second storage medium storing a second media ID identifying the second storage medium, wherein the right of using the contents stored in said first storage medium is devolved from said first storage medium to said second storage medium". Further, the first use information represents "a right to use the contents". In particular, the first encryption secure information is generated by encrypting the key and the first use information "with the first media ID". The license devolution apparatus comprises

decoding means for decoding **the first encryption secure information** stored in said first storage medium using the first media ID to obtain **the key** , and **the first use information**; and

encryption means for encrypting **with the second media ID the key and a second use information**, representing a **second right to use the contents that is devolved from the first storage medium to the second storage medium**, together with one another or individually with the second media ID, to generate **a second encryption secure information** for storage in said second storage medium.

These patentably distinguishing features have the benefit of providing a license devolution system which prevents access or use of contents (e.g., music, images, software products) on a recording media even if the key used to encrypt the contents (i.e., the predetermined key) and the contents are copied, because the media ID of the recording media on which the contents are copied, which is used by the decoding means to decode the predetermined key and use information, does not match the media ID of recording media used previously to encrypt the key and the contents.

The Examiner asserts that (using the recitation of claim 1 as an example) "a first storage medium storing contents encrypted with a predetermined key" in the present invention corresponds to the "enabler key" shown and disclosed in Ross, Fig. 6B; column 1, lines 46-51; FIG. 5; FIG. 2; column 6, lines 1-3, 8-13, 16 and 19-20. However, the present invention is similar to a video game machine cassette and the like in that when products are distributed from a factory, a media ID (i.e., information based on hardware or hardware manufacturing information) corresponding to a manufacturing number information is recorded on each of the recording media to be distributed. Further, similar to a video game machine cassette and the

like, utilization or use information (license) for a user is recorded on the media to be distributed. This is different from the process disclosed in Ross where a product licensing information, which is managed, is recorded on a recording medium (e.g., a disk of a personal computer) other than the recording media to be distributed. For example, Ross discloses that the enabler key is stored in an enabler key database that is shipped to a fulfillment agent, which manages the licensing information (*See* Ross, column 3, lines 25-27). In contrast, in the present invention, a license is recorded on the media to be distributed and is managed through an association with the media, such as the media ID.

Further, the "predetermined key" in the present invention is different from the enabler key disclosed in Ross. In contrast, the present invention provides a system and mechanism for limiting use or access to contents (which may be visuals and music, and in some cases, an application software) based upon double encryption. A simple encryption key, that is, the "predetermined key" referred to in the present invention is an encryption key common to the contents (i.e., all the contents on all the media to be distributed may be encrypted using the predetermined key). An object of the simple encryption key is to generate encrypted contents common to all the media to be distributed. An object of the double encryption is to encrypt the simple encryption key using media ID information, which would be different for each user. Thus, even if the simple encryption key is copied, it is very difficult, and perhaps impossible, to utilize the content because the media ID used to encrypt the simple encryption key would not match the media ID of the recording media on which the contents have been copied.

In Ross, the double encryption involves using a product serial number, which presumably is common to all of the products and not unique for each user. Further, the system in Ross, may also use information (e.g. random numbers), which is logically generated, as the encryption key for double encryptions. Thus, it is possible to duplicate such encryption key in Ross. In contrast to Ross, in the present invention hardware information, such as a manufacturing number of a recording medium, such as a magneto-optical disk, is utilized as an encryption key to achieve double encryption, making it very difficult and nearly impossible to duplicate the encryption key.

The Examiner also asserts that Ross discloses in column 1, lines 51-54, lines 37-38; and column 6, lines 40-49, 52-54 the feature of (using recitation of claim 1 as an example) "a second storage medium storing a second media ID identifying the second storage medium". In contrast to Ross, the license devolution apparatus according to the present claimed invention deals with a recording medium having hardware based information (i.e., media ID) which is not capable of being rewritten and erased (i.e., media ID areas 11 and 31 that are provided on a non-volatile or read-only storage medium, which is not rewritable physically). Further, license information is stored in a distributed recording medium and thus can be managed on an off line basis at a shop such as a video game machine shop without relying on communications through a network.

Dependent claims 2-7 (depending, either directly or indirectly, from claim 1) recite their own patentably distinguishing features and are also patentably distinguishing over the foregoing references at least due to their dependencies from independent claim 1.

For example, claim 2 recites the patentably distinguishing feature of "encryption means" that "encrypts with the first media ID a third use information, obtained through subtracting the second use information from the first use information" to "generate a third encryption secure information" and "stores the third encryption secure key in the first storage medium". This patentably distinguishing feature has the benefit of providing a license devolution system in which the license information is directly and securely (i.e., by using the media ID discussed above) stored in the medium to be distributed. Therefore, in the present invention the storage mediums are not read-only and may also be of the write-read type, such as a magneto-optical disk. In particular, each storage medium in the present invention stores three types of information, which include (using the recitation of claims 1 and 2 as an example) "contents encrypted with a predetermined key"; a "media ID" identifying the storage medium; and "encryption secure information". Further, the encryption secure information is generated by encrypting the "key" and "use information". The "use information" represents "a right to use the contents". Thus, unauthorized rewriting or alteration of the license information or management software of an end user is not easy in the present invention because of using

hardware or physical information (i.e., media ID) to encrypt, either together or individually, the predetermined key used to encrypt the content and the use information. On the other hand, the systems disclosed in Ross are independent of hardware information and therefore susceptible to easy falsification of license information.

Claim 3 recites the patentably distinguishing feature that “the key constituting the first encryption secure information stored in the first storage medium is destroyed”. This patentably distinguishing feature has the benefit of prohibiting the encryption key and the license association information from being read physically when the license becomes null and void. In particular, the present invention is directed to a license devolution system that accommodates identifying a devolution source and a devolution destination in accordance with hardware manufacturing information (i.e., media ID) corresponding to the media on which the contents are stored. Ross, however, does not disclose or suggest, as in the present invention, restricting access to contents of a media based upon hardware information associated with the license devolution, for example, at the time of registering end users. Therefore, in the systems disclosed in Ross the same user is permitted to have the same license in a plurality of storage-media. Accordingly, there is a possibility of unfair utility by the end users.

Withdrawal of the rejection of claims 1-7 and allowance of claims 1-7 and new claim 8 is respectfully requested.

Conclusion

In view of the amendments and remarks presented above, it is respectfully submitted that the application is in condition for allowance, and such action is hereby solicited.

If there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

Respectfully submitted,
STAAS & HALSEY LLP

By:


Mehdi Sheikerz

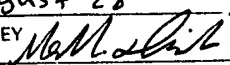
Registration No.: 41,307

700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001
(202) 434-1500

Date: August 28, 2000

CERTIFICATE UNDER 37 CFR 1.8(a)

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231

on August 28 2000
STAAS & HALSEY
By: 
Date August 28, 2000